Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

May 16, 2013

Media Contacts: Mike Rosen, Charlotte Sellmyer
(202) 226-8417

Statement of Subcommittee Chairman Patrick Meehan (R-PA)
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies
Committee on Homeland Security

"Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities"

Remarks as Prepared

I would like to welcome everyone to today's hearing, which will give members an opportunity to examine in-depth the work of the Department of Homeland Security's National Cybersecurity & Communications Integration Center (NCCIC).

The NCCIC is one of the U.S. Government's key civilian interfaces with the private sector for cyber threat information sharing, incident response, and protecting U.S. critical infrastructure.

The NCCIC is a collaborative method for federal agencies, state and local governmental entities, and the private sector to communicate cyber threat information, analysis, and prevention methods in real-time.

The Subcommittee has been crafting a body of work that will help to establish key areas where we can improve the Department's critical infrastructure protection from a cyber attack. We have examined the threat, particularly from nation-states. We have looked at protecting U.S. citizens from civil liberty violations. And today, we look at the threat mitigation capabilities at the Department of Homeland Security.

The Director of National Intelligence James Clapper testified before Congress this year, stating that cyber is the number one national security threat facing our country. On March 12th,

Director Clapper stated that "We assess that highly networked business practices and information technology are providing opportunities for foreign intelligence and security services, trusted insiders, hackers, and others to target and collect sensitive U.S. national security and economic data."

In addition, the Director for the National Security Agency, Keith Alexander has said that cyber espionage has caused the "greatest transfer of wealth in history".

Our nation is in a new era, and our security is no longer protected by oceans and borders. Indeed, American achievement in the 21st Century will be intricately tied to our ability to secure our networks; primarily our critical infrastructure networks.

While our military protects our nation from foreign adversaries, the security of our critical infrastructure – our economy, our roads and bridges, domestic energy, water and public utility systems – must be a collaborative effort between the private sector, and local, state, and federal government. We need a civilian agency to facilitate this partnership. And that agency is the Department of Homeland Security.

Today's hearing will give us an opportunity to hear from our expert panel regarding ways that the NCCIC currently brings a collaborative, national response to cybersecurity. Our capacity within the Committee on Homeland Security is to provide proper oversight to ensure that the NCCIC is functioning properly, and is capable of leading the protection of federal agencies in cyberspace; partnering with critical infrastructure owners and operators to share information and reduce risk; and providing the necessary intelligence elements to ensure that state and local critical infrastructure operators are mitigating cyber threats.

I am looking forward to hearing from our witnesses, particularly in areas that will help the committee as a legislative body strengthen the Department's capabilities.

We must examine ways to encourage increased participation from owners and operators of critical infrastructure. We need to ensure that the Department is successfully disseminating threat data with other federal agencies – in particular the Departments of Justice and Defense. And most importantly, we must make sure that there are sufficient privacy protections in place to ensure that the Department is able to anonymize data for both personally identifiable information, and stakeholder identifiable information.

I look forward to hearing from our panel.

###